UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/499,736	02/08/2000	Pierre Calvez	T2147-906343	1674

7590 11/18/2004

Miles & Stockbridge PC.
1751 Pinnacle Drive
Suite 500
Mclean, VA 22102-3833

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/499,736	CALVEZ ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *29 and 30* is/are allowed.

6)☒ Claim(s) *15-28 and 31-35* is/are rejected.

7)☒ Claim(s) *22 and 24-26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 May 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 15-35 are pending.

2. Claims 29 & 30 are allowed.

Drawings

3. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are informal, containing crossed-out and handwritten text. The proposed drawing corrections of May 31, 2000 have been accepted; formal drawing are required. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Objections

4. Claims 22 & 24-26 is objected to because of the following informalities: "wherein said at least one shared secret or secrets, as the case may be" should be replaced with "wherein said at least one shared secret". Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 15-23, 27-28 & 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the SKID protocol, described in Applied Cryptography, Second Edition, by Bruce Schneier, published 1996, in view of U.S. Patent 6,014,085 to Patel, in further view of U.S. Patent 6,401,204 to Euchner et al. (Euchner).

Regarding claims 15, 27 & 28, Schneier discloses Alice being a user/local machine and Bob being a host/server (p. 52, ¶1 and p. 55, ¶1). Schneier discloses creating a challenge/random number and communicating it along with elements known by the user/"A" to the server/"B" (p. 55, step 1 and p. 56, step 3). Schneier discloses performing a calculation/hash, obtaining a first response/R_B,$H_k(R_A,R_B,B)$ and transmitting that response (p. 55, step 2) to the user/"A" by the server/"B"/administrator. Schneier discloses performing a second calculation/hash that is a function of predetermined data and comparing the results (p. 56, step 3). Schneier lacks the challenge including information representing the type of challenge. However, Patel teaches that to avoid replay attacks in an authentication system, it is beneficial to use challenge codes representing different challenge types to determine authentication codes (col. 5, lines 5-36) and that one type of challenge code is a version number (col. 6, lines 39-66). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a version number and information indicating the type of challenge. One of ordinary skill in the art would have been motivated to perform such a modification to prevent impersonators from successfully realizing replay attacks, as taught by Patel (col. 5, lines 5-36 & col. 6, lines 39-66). As modified, Schneier lacks the challenge type indicating whether a network authentication has been performed. However, Euchner teaches that in an authentication protocol (col. 2, lines

26-33), a count value is included in the messages to distinguish between different protocol runs for the same connection (col. 6, line 66 – col. 7, line 6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to indicate whether a network authentication has been performed. One of ordinary skill in the art would have been motivated to perform such a modification to distinguish between different protocol runs, as taught by Euchner (col. 2, lines 26-33 & col. 6, line 66 – col. 7, line 6).

Regarding claims 16-18, Schneier discloses a hash being performed over the challenge/random number and at least one secret/k (p. 55, step 2 and p. 55, step 3).

Regarding claims 19-21, Schneier, as modified above, lacks the act of sharing a secret value. However, Schneier teaches that "In general, a man-in-the-middle attack can defeat any protocol that doesn't involve a secret of some kind." Schneier further teaches that protocols that combine authentication with key exchange solve a general computer problem wherein different users want to communicate securely (p. 56, 2nd paragraph). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a secret key between the local machine and server to enable secure communication after authentication. One of ordinary skill in the art would have been motivated to perform such a modification to enable secure communication and to secure the transaction from the man-in-the-middle attack, as taught by Schneier.

Regarding claim 22, Schneier, as modified above, lacks modifying a shared secret with a key that depends on the local machine. However, in a discussion of key-exchange protocols, Schneier discloses that public key cryptography makes key exchange easier, in that a first party encrypts a secret with the public key of a second party. This allows only the second party access

to the secret (p. 48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the shared secret with a key that depends on the local machine to make key exchange easier. One of ordinary skill in the art would have been motivated to perform such a modification to make key exchange easier, as taught by Schneier (p. 48).

Regarding claim 23, Schneier discloses a byte string consisting of hashing a Master Station Secret/R_A to obtain a Station Secret/$H_k(R_A,R_B,B)$ (p. 55, step 2).

Regarding claim 31, Schneier discloses a response/$H_k(R_A,R_B,B)$ composed of hashing a string composed of a user's password/K, a Station Secret/R_A and the user name/B (p. 55, step 2).

Regarding claim 32, Schneier discloses a response/$H_k(R_A,R_B,B)$ composed of hashing a string composed of a fixed security key/K stored in the local machine/B and server/A, the name of the local machine/B (p. 55, step 2).

7. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,161,185 to Guthrie et al. (Guthrie) in view of Patel in further view of Euchner. Guthrie discloses a user (Fig. 5, element 114), local machine (Fig. 5, element 102) and remote server (Fig. 5, element 104), means for classifying information (Fig. 5, element 120) and communication means (Fig. 5, element 112 & 118). Guthrie further discloses a system administrator (col. 2, lines 42-47), a local machine comprising an authentication module that include a first user module (Fig. 5, element 126) for generating a challenge (Fig. 4, element 114) and second user module for generating a response (Fig. 5, element 130) and an administrative authentication module for authorizing access (Fig. 5, element 132). Guthrie lacks the challenge

including information representing the type of challenge. However, Patel teaches that to avoid replay attacks in an authentication system, it is beneficial to use challenge codes representing different challenge types to determine authentication codes (col. 5, lines 5-36) and that one type of challenge code is a version number (col. 6, lines 39-66). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a version number and information indicating the type of challenge. One of ordinary skill in the art would have been motivated to perform such a modification to prevent impersonators from successfully realizing replay attacks (col. 5, lines 5-36 & col. 6, lines 39-66). As modified, Guthrie lacks the challenge type indicating whether a network authentication has been performed. However, Euchner teaches that in an authentication protocol (col. 2, lines 26-33), a count value is included in the messages to distinguish between different protocol runs for the same connection (col. 6, line 66 – col. 7, line 6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to indicate whether a network authentication has been performed. One of ordinary skill in the art would have been motivated to perform such a modification to distinguish between different protocol runs, as taught by Euchner (col. 2, lines 26-33 & col. 6, line 66 – col. 7, line 6).

8. Claims 24, 25 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Patel & Euchner, as applied to claims 16, 17 & 18 above, in further view of U.S. Patent 5,081,677 to Green et al. (Green). Schneier, as modified above, lacks a version number associated with a shared secret, and incremented when the shared secret is modified. However, Green teaches that, when updating a master key, it is useful to associate a version

number with a the key and to increment the version number when the key is modified, to enable distributed copies of the key to be updated on first use and to modify the master key without exposing it to applications (col. 2, lines 30-67 & col. 3, lines 5-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to associate a version number with a shared secret and to increment the version number when the secret is modified. One of ordinary skill in the art would have been motivated to perform such a modification to enable the shared secrets to be updated at different times (on first use) and to enable modification of the secret without exposing it, as taught by Green (col. 2, lines 30-67 & col. 3, lines 5-35).

9. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Patel & Euchner, as applied to claim 15 above, in view of U.S. Patent 5,774,650 to Chapman et al. (Chapman). Schneier, as modified above, lacks temporary authorization where the duration is configurable. However, Chapman teaches time-limited access to a system is beneficial to temporarily enable a privileged user to use the full performance capability of a system by temporarily denying access to less-privileged users (col. 2, lines 38-61). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a time-based authorization in Schneier's system to enable a privileged user to access the full capabilities of the system. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of enabling a user to temporarily gain full access to a system's resources, as taught by Chapman (col. 2, lines 38-61).

10. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Patel & Euchner, as applied to claim 15 above, in view of Windows NT User Administration, by Ashley J. Meggitt & Timothy D. Ritchey (Meggitt). Schneier, as modified above, lacks specific disclosure of locally authenticating a user after disconnection. However, Meggitt teaches that Windows NT allows a user, normally authenticated through a domain, to login to a local workstation even if the roaming profile is unavailable (p. 139). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the authentication protocol taught by Schneier to allow login to a local machine by a user, usually authenticated remotely, in the case that network connectivity has been disrupted. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of local system access even when remote authentication is unavailable, as taught by Meggitt (p. 139).

Allowable Subject Matter

11. Claims 29 & 30 are allowed.

12. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 29 & 30, the prior art relied upon fails to specifically teach the limitation of a challenge composed of a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed; second and third bytes representing the version number of the shared information; and random alphanumeric characters of the fourth to twelfth bytes.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
November 9, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100